Wrocław University of Science and Technology

Multi-antenna system as an eavesdropper for directional beams

Adam Narbudowicz

adam.narbudowicz@pwr.edu.pl

HR EXCELLENCE IN RESEARCH

Wroclaw University of Science and Technology

Copyright

Wroclaw University of Science and Technology

Abstract

The presentation discusses the use of MIMO system as an eavesdropper in directional wireless communication. The proposed theoretical attack model involves collusion of signal gather from multiple antennas that are located in specific location within area under control of the eavesdropper. The attack shows, that – under some circumstances – the attack can intercept signal from directional beam, even without placing eavesdropper's antennas within the beam. Additional, the attack makes ineffective artificial noise techniques that are often used to increase physical layer security.

Keywords: physical layer security, directional modulation, artificial noise, MIMO, antenna array

Wrocław University of Science and Technology

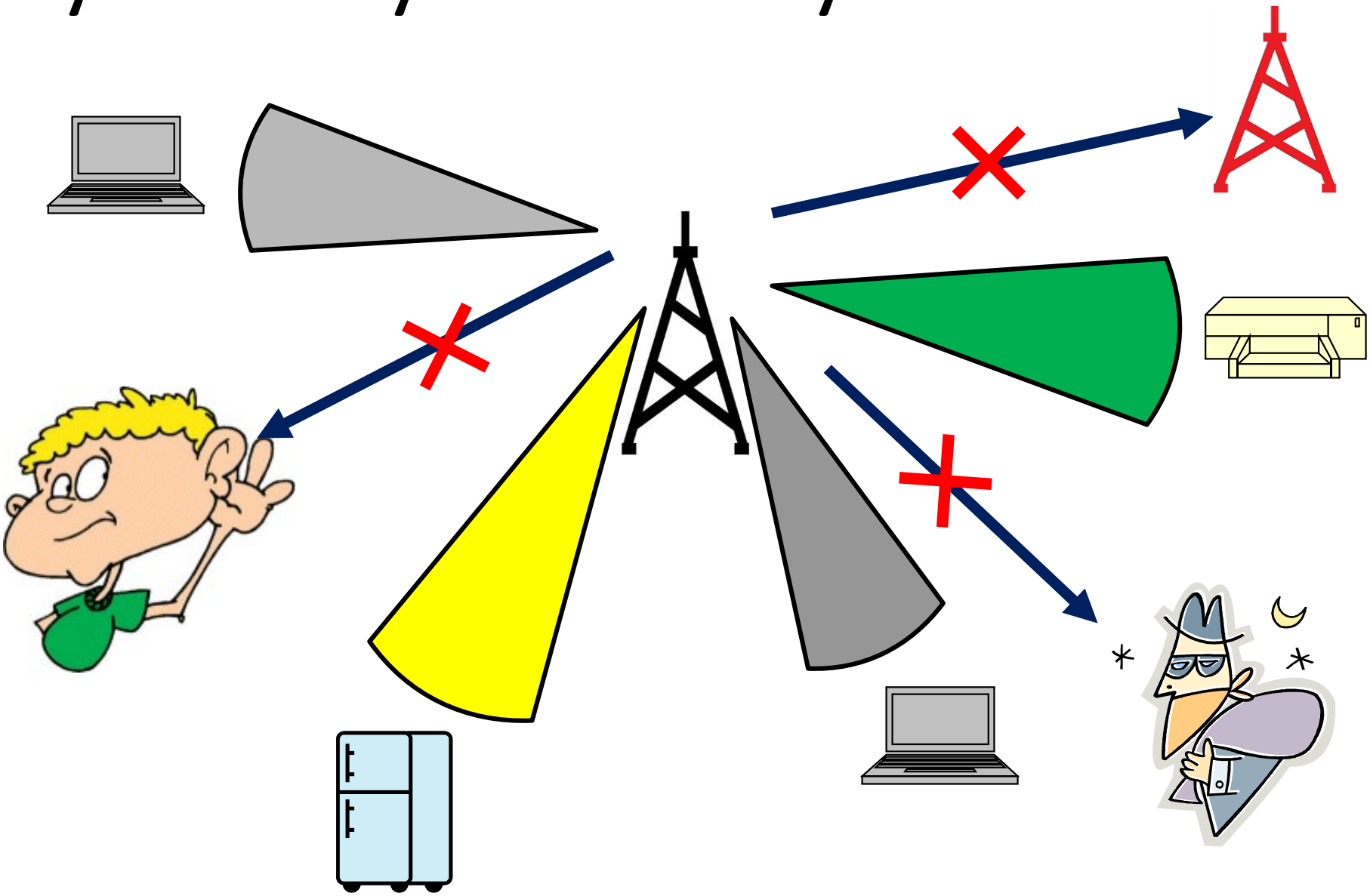
Adam Narbudowicz is an Assistant Professor at Wroclaw University of Science and Technology, Poland and SFI Starting Investigator at Trinity College Dublin, Ireland working within CONNECT Research Centre. He received habilitation (DSc) in 2020 from Wroclaw University of Science and Technology, PhD in 2013 from Dublin Institute of Technology (now TU Dublin), Ireland and M.Sc. in 2008 from Gdansk University of Technology, Poland. In 2014 – 2019 he was a postdoctoral research fellow at Technological University Dublin, leading various research projects including EDGE Postdoctoral Research Fellow at CONNECT Research Centre. In 2014 – 2017 was awarded Irish Research Council and Marie-Curie Action co-funded ELEVATE fellowship to work at he worked at RWTH Aachen University, Germany.

His research interests include physical layer security, compact antennas with beamforming and CubeSat antennas. Dr Narbudowicz was awarded Scholarship for Outstanding Young Scientists by Ministry of Science and Higher Education of Poland in 2019, the inaugural 2018 Prof Tom Brazil CONNECT Excellence in Research Award, Best Paper Award during ISAP 2017 conference, best poster by popular vote during 2018 IEEE -EURASIP Summer School on Signal Processing; and DIT Inventor Competition Award for Best Postgraduate/Staff Invention in 2012. Since January 2020 he serves as a vice-chairman of the IEEE Poland APS/MTT/AES joint chapter.

HR EXCELLENCE IN RESEARCH

Wrocław University of Science and Technology

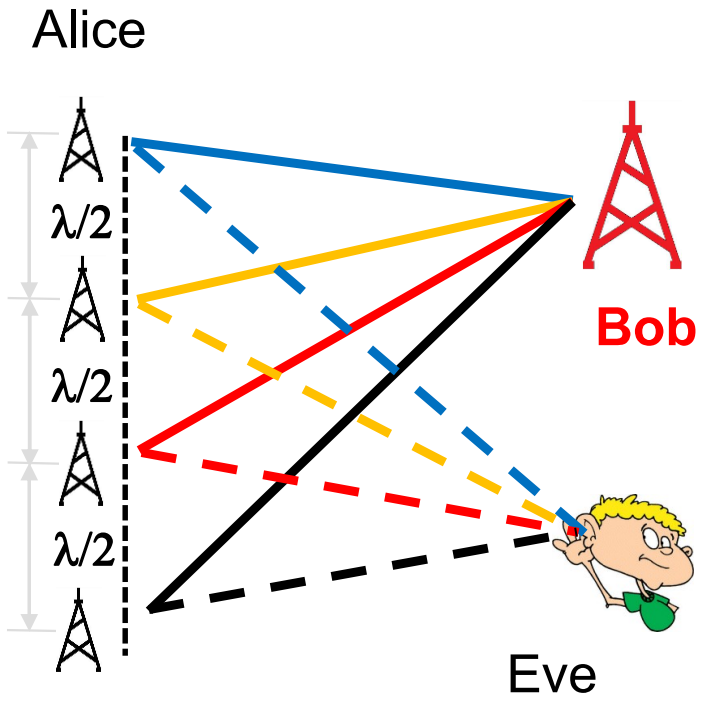
Physical Layer Security



Wroclaw University of Science and Technology

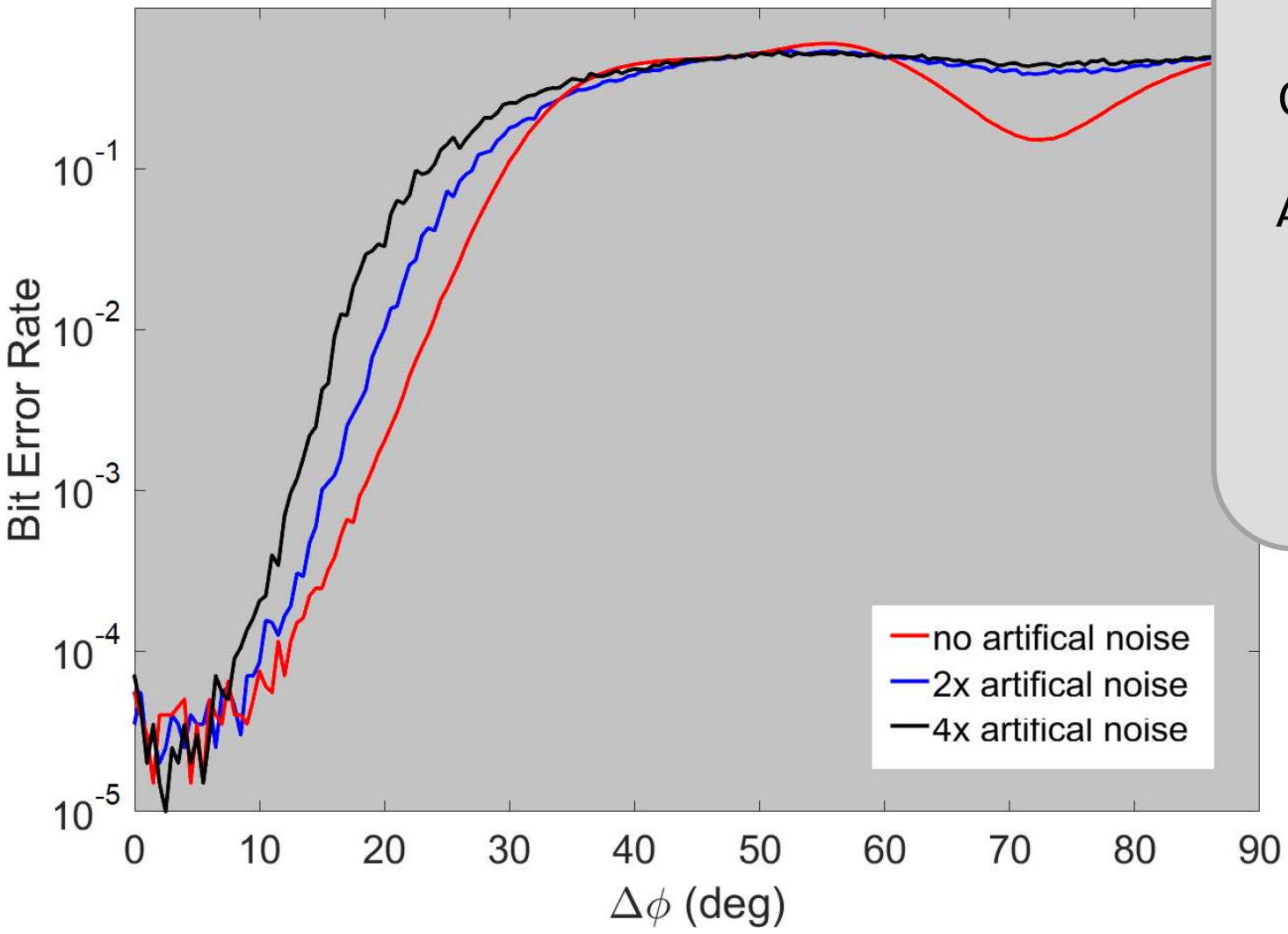
Artificial noise

- Takes the advantage of directional beams
- Mainly discussed in the context of mm-Waves and MIMO
- The Tx array (Alice) transmits legitimate signal with antenna coefficients adjusted for the maximum at legitimate receiver (Bob)
- Simultaneously, Alice transmits artificial noise with antenna coefficients adjusted for the null at the legitimate receiver
- The artificial noise will be observed by any receiver with channel coefficient different from Bob's channel



Wroclaw University of Science and Technology

Artificial noise



BER for Eve

Bob at 0 deg.

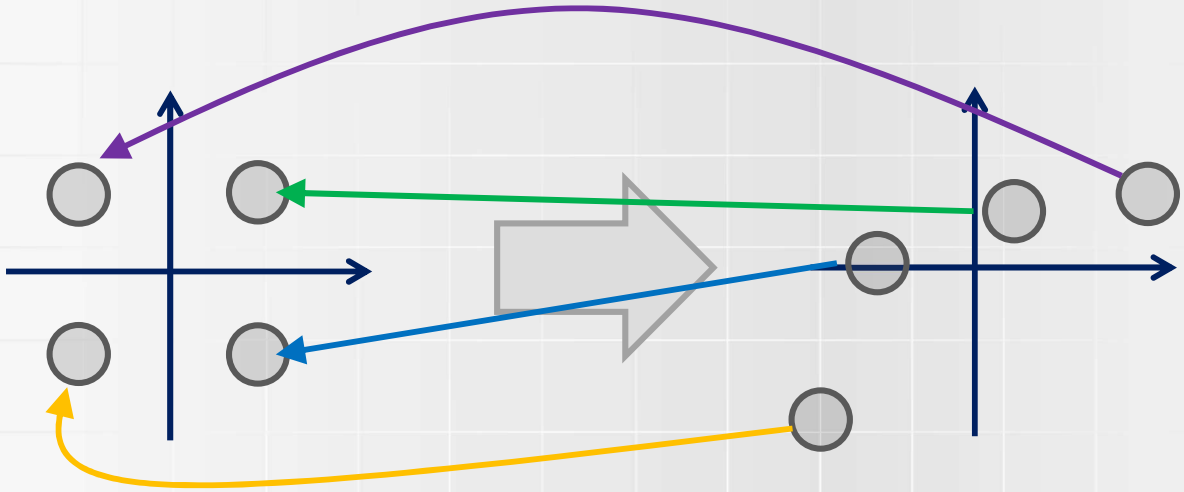
QPSK modulation

Alice: 4 antennas

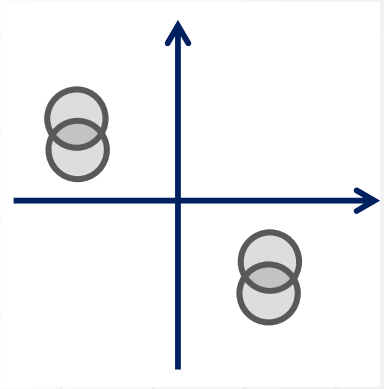
Eve: 1 antenna

SNR = 12 dB

Known symbol attack



Constellation scatters, but:
– No security if points can be mapped to their original locations



Desired security features:

- Decrease distance between points
- Noise is an ally
  (closer points – more prone to noise)
- Keyless technique – transmitter can change scattering whenever it wishes to without affecting legitimate receiver

Wroclaw University of Science and Technology

Proposed MIMO attack

- Directional beam from antenna array (Alice) that uses artificial noise can be modelled as a MISO system:

$$R_{bob} = C_{bob}\, T + n$$

R – received signal by Bob
C – Bob's channel vector (each Alice's antenna -> Bob)
T – transmitted signals vector (secret message)
n – noise ('natural', uncorrelated)

But… what if eavesdropper also uses many antennas?

- Channel ***C*** changes with physical location
  ➔ Eve's channel is different ($C_{eve} \neq C_{bob}$)

- However, if EVE has as many antennas as Alice,
  Eve can build a set of equations to figure out ***T***

Wrocław University of Science and Technology

Proposed MIMO attack

$$\boldsymbol{R}_{bob} = \boldsymbol{C}_{bob}\ \boldsymbol{T} + \boldsymbol{n}$$

How to intercept the message?

R – received signal by Bob
C – Bob's channel vector (each Alice's antenna -> Bob)
T – transmitted signals vector (secret message)
n – noise ('natural', uncorrelated)

A – no. of antennas used by Alice

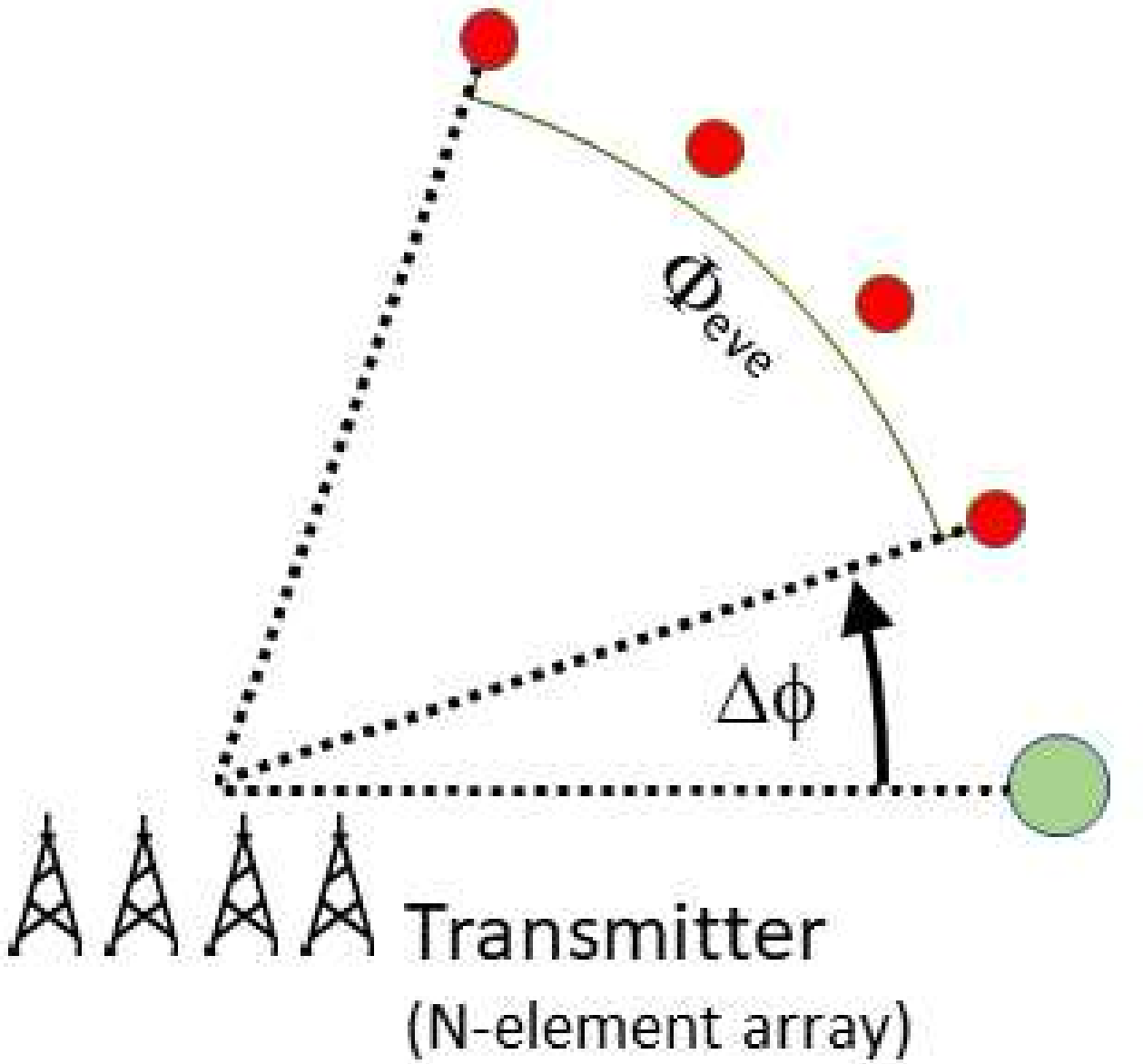
- Eve samples *A* locations, each with different channel $\boldsymbol{C}_{eve}$
- Eve records received signals as *A*-long vector $\boldsymbol{R}_{eve}$
- Assuming channels $\boldsymbol{C}_{eve}$ *and* $\boldsymbol{C}_{bob}$ can be estimated (realistic for line-of-sight)

Eve calculates:

$$\hat{\boldsymbol{T}} = \boldsymbol{C}_{eve}^{-1}\boldsymbol{R}_{eve} = \boldsymbol{T} + \boldsymbol{C}_{eve}^{-1}\boldsymbol{n}_{eve}$$

Wrocław University of Science and Technology

Modelling

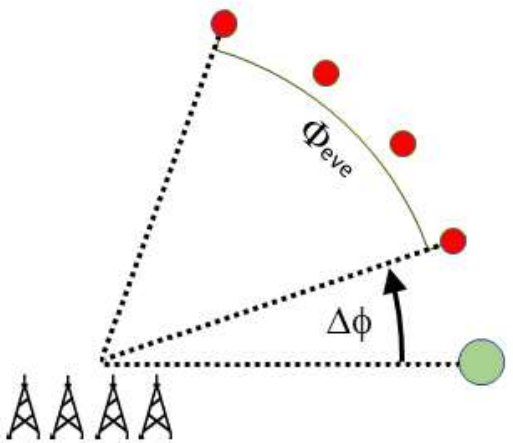


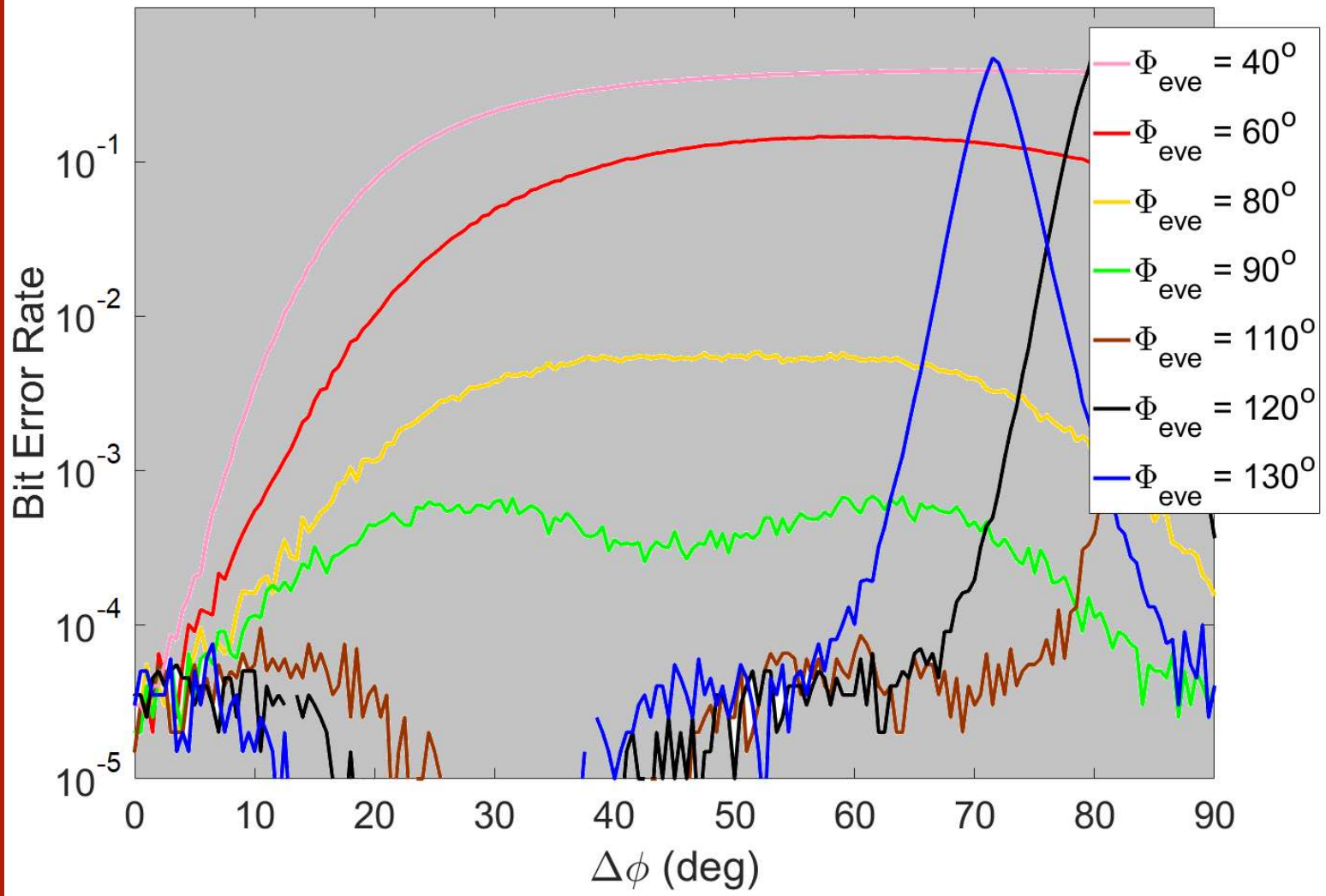
Wroclaw University of Science and Technology

Assumptions

- Eve has knowledge about all propagation channels involved (Alice -> Bob and Alice -> Eve)
- Eve and Alice use the same number of antennas and same antenna type - omnidirectional.
- Eve can perfectly synchronise its antennas
- Line-of-sight channel model is involved
- The demodulation is executed by mapping the processed signal to the nearest symbol of QPSK

Simulation: 4 antennas





BER for Eve

Bob at 0 deg.

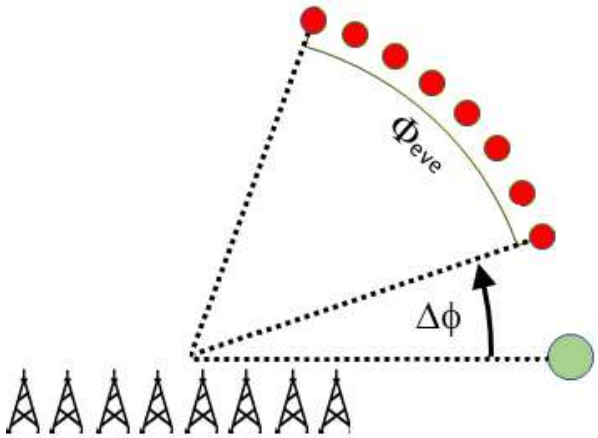
QPSK modulation

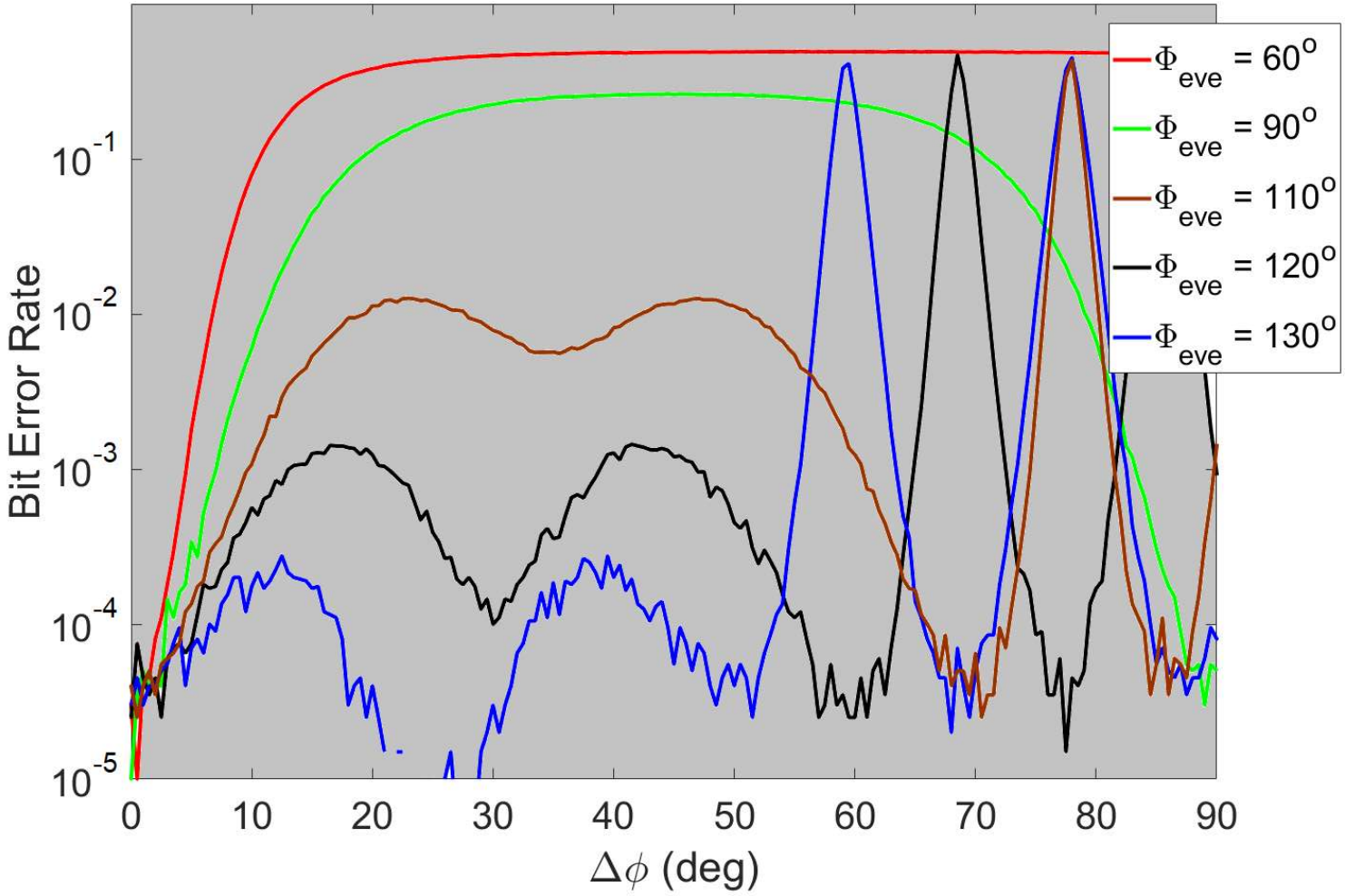
4 antennas

SNR = 12 dB

Wroclaw University of Science and Technology

Simulation: 8 antennas





BER for Eve

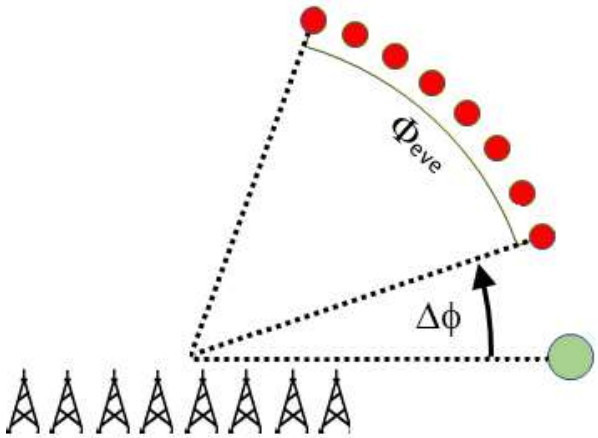
Bob at 0 deg.

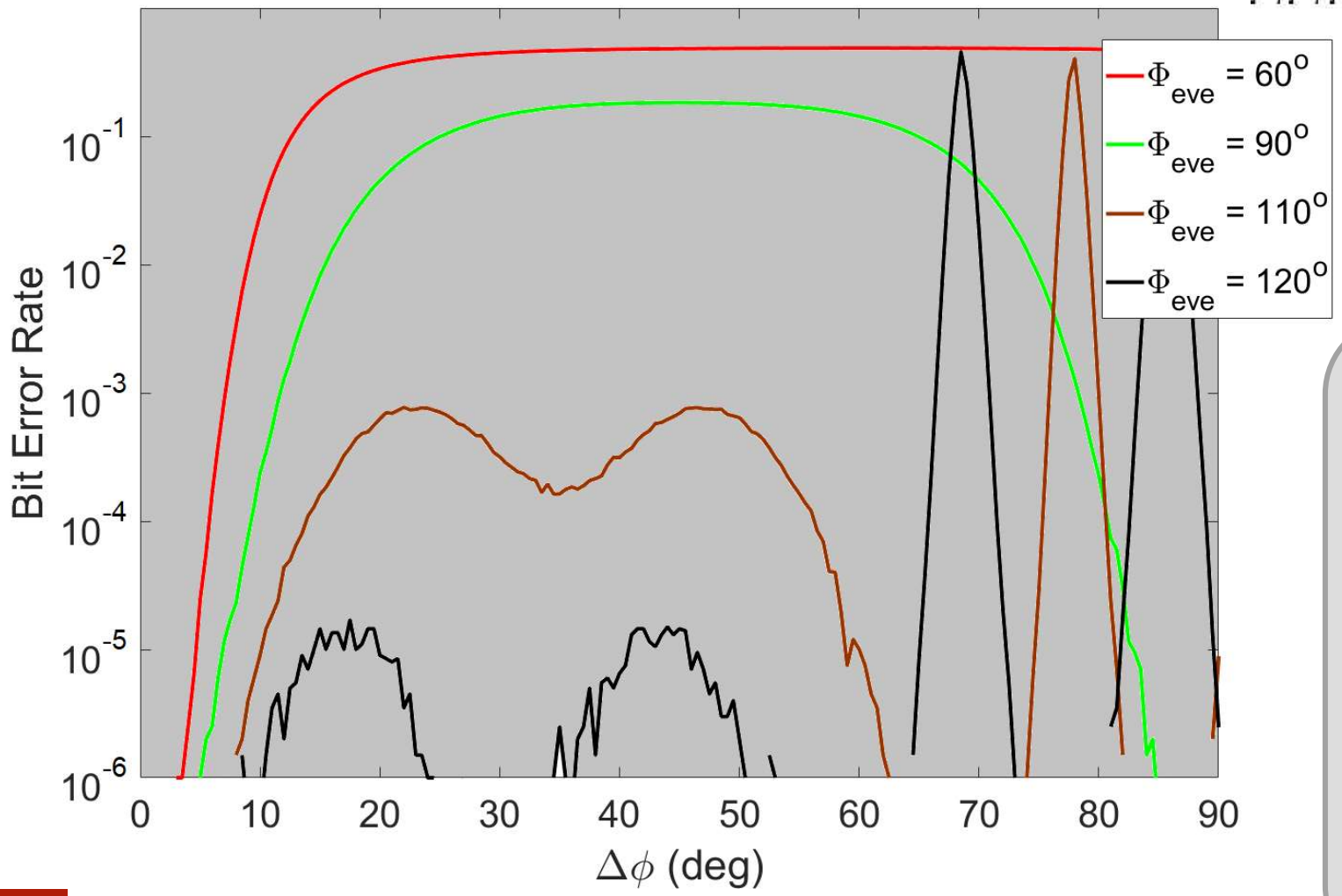
QPSK modulation

8 antennas

SNR = 12 dB

Simulation: 8 antennas





BER for Eve

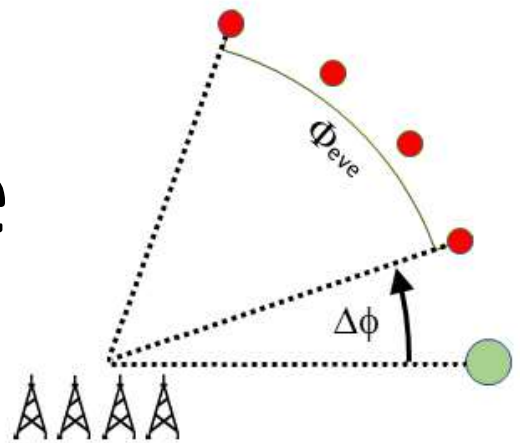
Bob at 0 deg.

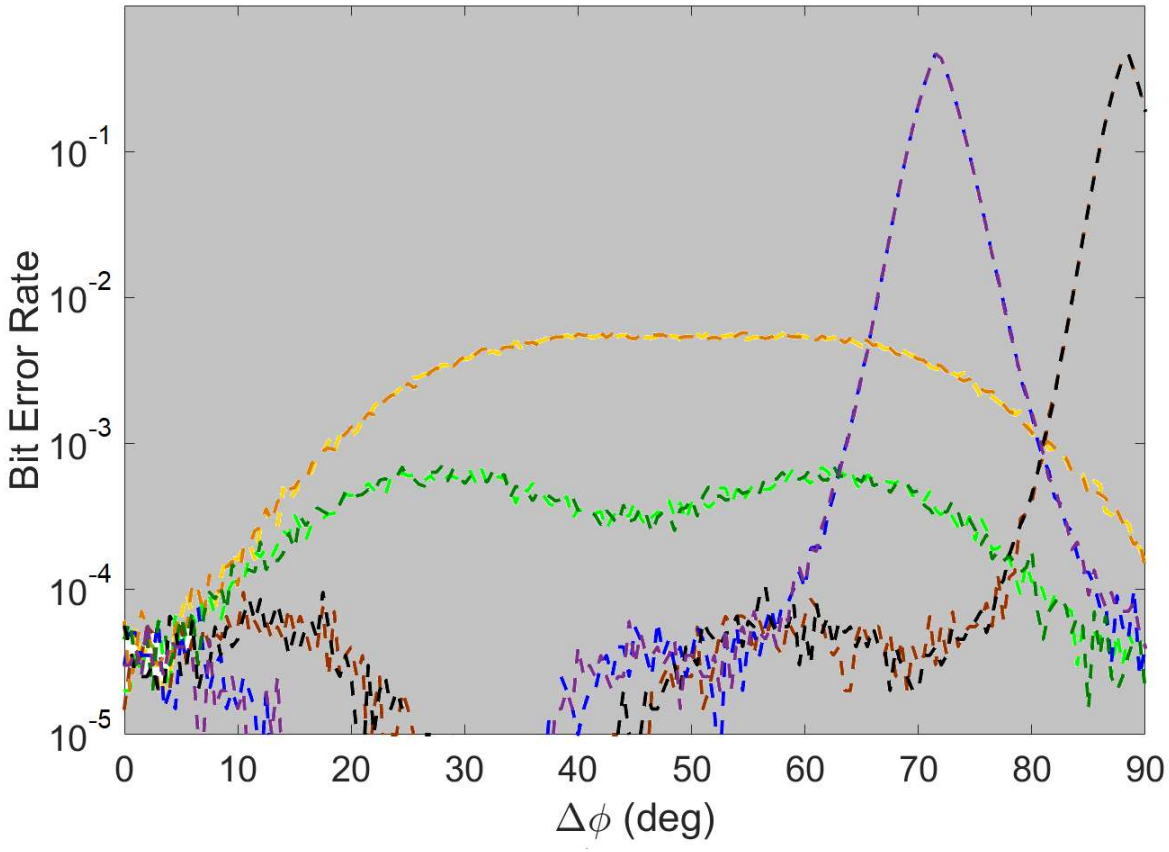
QPSK modulation

8 antennas

SNR = 15 dB

Simulation: artificial noise





BER for Eve

Bob located at 0 deg.

QPSK modulation

4 antennas

SNR = 12 dB

No artificial noise

- $\Phi_{eve} = 80^o$
- $\Phi_{eve} = 110^o$
- $\Phi_{eve} = 90^o$
- $\Phi_{eve} = 130^o$

4x artificial noise

- $\Phi_{eve} = 80^o$
- $\Phi_{eve} = 110^o$
- $\Phi_{eve} = 90^o$
- $\Phi_{eve} = 130^o$

Artificial noise has no effect on Eve!

Wroclaw University of Science and Technology

Conclusions

- Proposed attack where eavesdropper uses multiple antennas to intercept signal from multiple locations
- The attack is less efficient, as each eavesdropper's antenna experience uncorrelated noise
- However, the attack overcomes 'artificial noise' injected by Alice, as such noise is correlated between various locations
- Size of eavesdropper-controlled area is crucial

Wroclaw University of Science and Technology

References

- J. Ma et al., "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, pp. 89-93, Nov. 2018
- Y. Ju, Hui-Ming Wang, Tong-Xing Zheng, Q. Yin, and M. H. Lee, “Safeguarding Millimeter Wave Communications Against Randomly Located Eavesdroppers,” *IEEE Trans. On Wireless Communications*, vol. 17, no. 4, pp. 2675-2689, Apr. 2018
- Y. Zhu, L. Wang, Kai-Kit Wong, and R. W. Heath, Jr., “Secure Communications in Millimeter Wave Ad Hoc Networks,” *IEEE Trans. On Wireless Communications*, vol. 16, no. 5, pp. 3205-3217, May 2017
- M. P. Daly, E. L. Daly, and J. T Bernhard, "Demonstration of directional modulation using a phased array", *IEEE Trans. on Antennas and Propagation*, vol. 58, no. 5, pp. 1545-1550, May 2010
- Yuan Ding, and V. Fusco, "A Synthesis-Free Directional Modulation Transmitter Using Retrodirective Array", *IEEE Journal of Selected Topics in Signal Processing*, vol. 11, pp. 428-441, 2017
- A. Narbudowicz, M. J. Ammann, and D. Heberling, “Directional Modulation for Compact Devices”, *IEEE Antenna and Wireless Propagation Letters*, vol. 16, pp. 2094 – 2097, 2017
- T. R. Dean and A. J. Goldsmith, "Physical-Layer Cryptography Through Massive MIMO", *IEEE Trans. on Information Theory*, vol. 63, no. 8, pp. 5419-5436, Aug. 2017
- Yuan Ding, A. Narbudowicz, “Can Frequency Diverse Array Prevent Wireless Eavesdropping in Range Domain?”, arXiv:1910.02324

Wrocław
University
of Science
and Technology

Thank you

Contact:
adam.narbudowicz@pwr.edu.pl

HR EXCELLENCE IN RESEARCH